APR 05 2020 SUNDAY
Wk 14 (096-270)

Chapter - 6

Elliptic Curve.

Elliptic curve cryptography is the newest member of the 3 families of PK-algorithms. ECC provides the same level of security of RSA or DL systems with considerably shorter operands (160-256 vs 1024-3072 bits)

Introduction

Based on the generalised DLP and thus DL-protocols such as DH key exchange can be realised using elliptic ~~curves~~ keys.

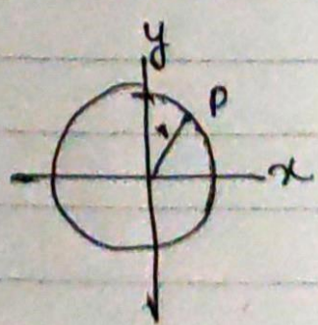
- look back at table:- 80bit block cipher RSA needs 1024 bits to get the same level of security RSA 3000-bits is way too slow.

Idea: Can we find another cyclic group in which the DLP is difficult?

Ideally ~~to~~ more difficult than Z_p^*

looking up at polynomials

$$x^2 + y^2 = r^2$$

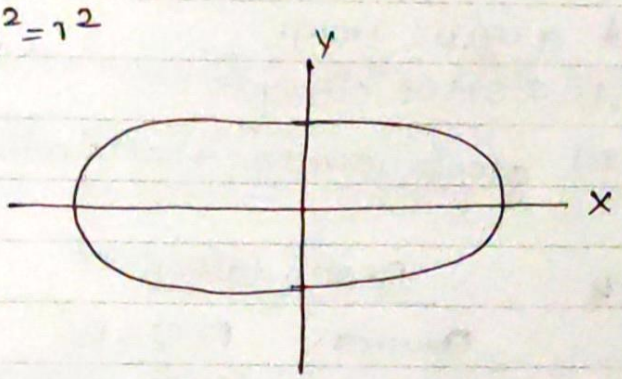


"Teach this triple truth to all: A generous heart, kind speech, and a life of service and compassion are the things which renew humanity."

plot all the pairs (x,y) which fulfill this equation in a coordinate system we obtain a circle.

$x \rightarrow$ not in circle, $\therefore$ does not satisfy the equation.

$ax^2+by^2=1^2$



obtain an ellipse.

- Both these are over $\mathbb{R}$
- For we in crypto we need to consider polynomials over Z_p.

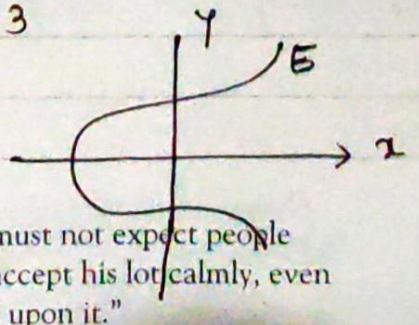
Def 6.1:- The elliptic curve over Z_p, $p>3$ is the set of all pairs $(x,y) \in Z_p$ which fulfill

$$y^2 \equiv x^3+ax+b \bmod p$$

together with an imaginary point of infinity $\mathcal{O}$ where $a,b \in Z_p$ and the condition

$$4a^3+27b^2 \neq 0 \bmod p.$$

Example 6.1:- $y^2 \equiv x^2-3x+3$



"Anyone who proposes to do good must not expect people to roll stones out of his way, but must accept his lot calmly, even if they roll a few stones upon it."

APR 07 2020 TUESDAY

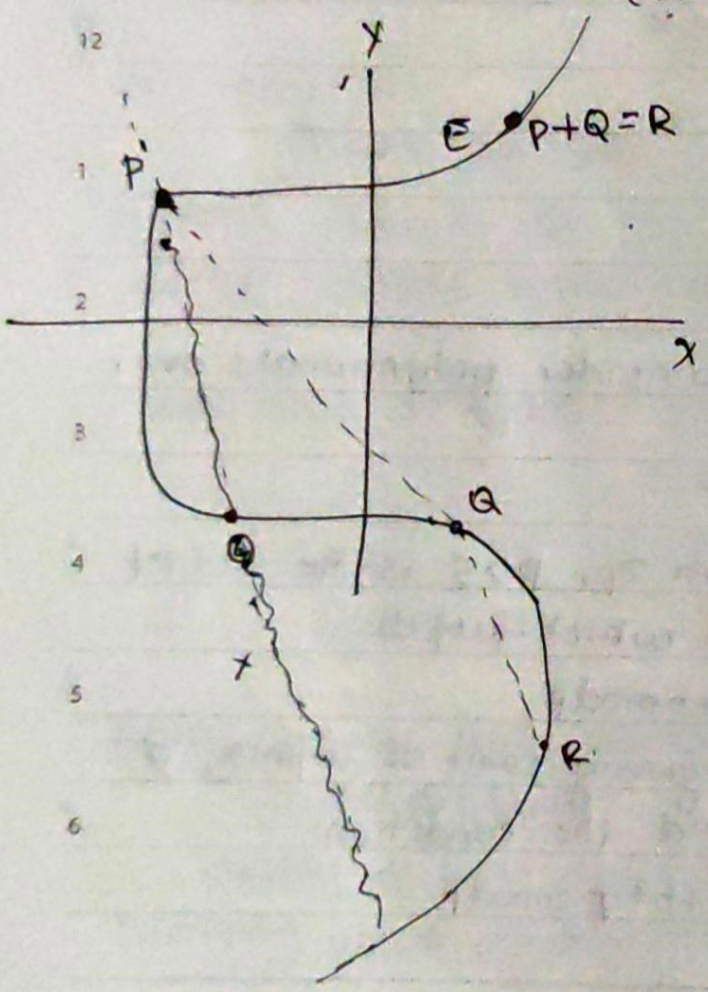
Wk 15 (098-268)

we study curves over Z_p. However, if we plot an EC over Z_p we do not get a curve. So we plot in $\mathbb{R}$.

$$y = \pm\sqrt{x^2 - 3x + 3}$$

Symmetric to the x-axis.

- for a DLP we need a cyclic group
  - (i) a set of elements
  - (ii) group operation that fulfill the group



Point addition:-

Question:- $P + Q = R$

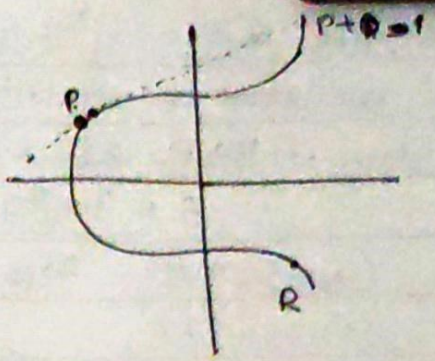
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

Given two points you compute line through P and Q, you get a third point and mirror it (x-axis)

"Set your heart on doing good things. Do it over and over again, and you will be filled with joy."

Point Doubling:- P+P.

Draw the tangent line and get a 2nd point of intersection and mirror.

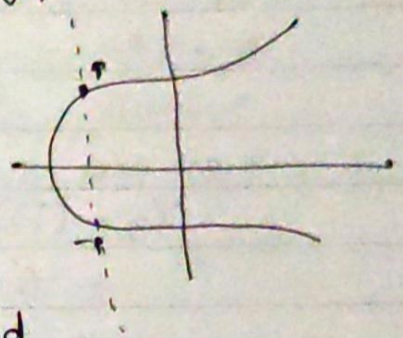


what is the neutral element $P + ? = P \quad \forall P$

No point on this curve exists.

we define a "point of infinity"

$P + (-P) = \mathcal{O}$



The question is how do we find $-P$?

if apply the tangent and chord method from above inverse of P is $(x_A - y_P)$

How do phones do this?

The curves point addition and point doubling

$$x_3 = s^2 - x_1 - x_2 \bmod p$$

$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$

$$s = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \bmod p & \text{if } P \neq Q \text{ addition} \\ \dfrac{3x_1^2 + a}{2y_1} \bmod p & \text{if } P = Q \text{ doubling} \end{cases}$$

"A good deed is never lost. He who plants kindness, gathers love; pleasure bestowed on a grateful mind was never sterile, but generally gratitude begets reward."

APR 09 2020 THURSDAY
Wk 15 (100-266)

→ going home yipee.

$$\begin{array}{r} 3 \\ 17\times5 \\ \hline 85 \\ 17\times9 \\ \hline 146 \end{array}$$

Example 6.2:- $y^2 \equiv x^3 + 2x + 2 \bmod 17$.

we want to double $P = (5,1)$

$P + P = 2P = (5,1) + (5,1) = (x_3, y_3)$

$$s = \frac{3x_1^2 + a}{2y_1} = \frac{3(5)^2 + 2}{2.1} \bmod 17.$$

$$= (2.1)^{-1} \cdot 9 \bmod 17$$

$$= 2^{-1} \cdot 9 \bmod 17.$$

$\because 2x \equiv 1 \bmod 17$, $x = 9$

$$= 9.9 \bmod 17$$

$$\equiv 13.$$

$x_3 = (13)^2 - 5 - 5 \bmod 17$

$= 6 \bmod 17$

$=$

$y_3 = (13)(5-6) - 1 \bmod 17$

$= (-13)(-1) \bmod 17$

$= 3 \bmod 17$

$2P(6,3)$

$$\begin{array}{r} -14 \\ +17 \\ \hline \end{array}$$

Check

$3^2 \equiv 6^3 + 2\times6 + 2 \bmod 17$

Theorem 6.1: The points on an EC together with $\mathcal{O}$ hay cyclic subgroups. Under certain conditions all points on an EC form a cyclic group.

"There is a sort of gratification in doing good which makes us rejoice in ourselves"

Example 6.8:- $y^2 \equiv x^3 + 2x + 2 \bmod 17$

(5,1) This is generator

All points on the curve form a cyclic group and the order is 19.

$P = (5,1)$	$6P = (16,13)$	$11P = (13,10)$	$16P = (10,11)$
$2P = (6,3)$	$7P = (0,6)$	$12P = (0,11)$	$17P = (6,14)$
$3P = (10,6)$	$8P = (13,7)$	$13P = (16,4)$	$18P = (5,16)$
$4P = (3,1)$	$9P = (7,6)$	$14P = (9,1)$	$19P = \emptyset$
$5P = (9,16)$	$10P = (7,11)$	$15P = (3,16)$	$20P = P$
			$21P = 2P$.

$19P = 18P + P$

$= (5,16) + (5,1)$ In crypto $\emptyset$ is ∞

$$s = \frac{y_2 - y_1}{x_2 - x_1} \bmod p$$

$$= \frac{16-1}{5-5} \bmod 17$$

$= 15 \cdot 0^{-1} \bmod 17$

$= \emptyset$

$18P = (5,16)$ ← equivalent modulo 17

$18P = (5,-1)$

$-P$

"Every man feels instinctively that all the beautiful sentiments in the world weigh less than a single lovely action taken to help others."

APR 11 2020 SATURDAY

Wk 15 (102-264)

Note: $P=(x_P, y_P)$

$-P=(x_P, -y_P)$

$19P = 18P+P$

$=(5,16)+(5,1)$

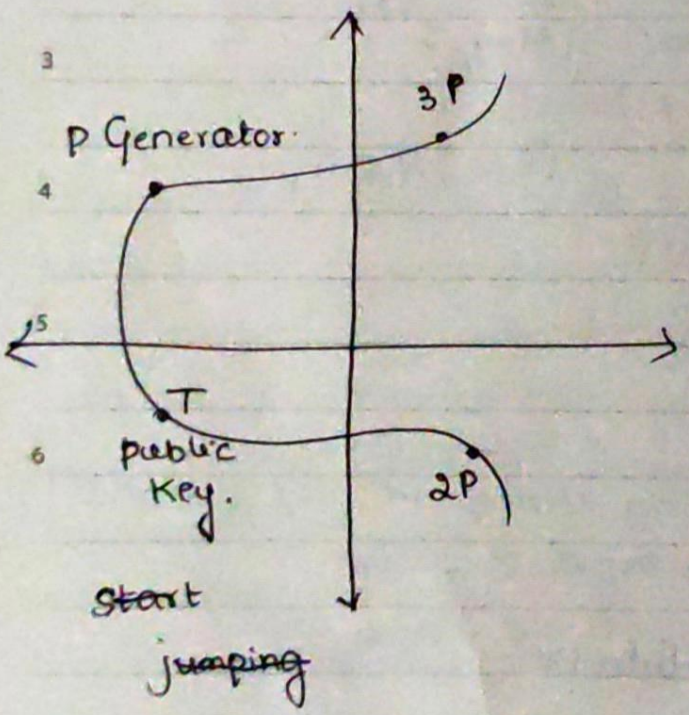
$-P+P=\emptyset$

$(5,16)$ inverse of $(5,1)$

Def 6.2: Elliptic curve DLP (ECDLP)

Given an elliptic curve E. we consider a primitive element P another element T. The DLP if finding another d, where $1 \le d \le \#$ E. Such that

$\underbrace{P+P+\dots+P}_{d \text{ times.}} = dP = T$



Start jumping / hoping around the curve and stop at some point T.

"The medical profession is directly related to one's life, those who are doing it for the sake of people without any profit motive are doing the best deed."

Given a start point P and final point T. you tell me how many times I jumped. The number of jumps is the private key.

Example 6.3:- Let's say $P=(5,1)$ and $T=(16,H)$

$T=(16,H)=dP$ what is d ?

$(16,H)=d(5,1)$ $\quad d=13.$

Note!-

$K_{pr}=d \leftarrow$ integer

$K_{pub}=T \leftarrow$ point on curve (groupelement).

Q:- what is #E ?

Cardinality of the group

previous example it was 19 points.

Theorem 6.2: Hasse's Theorem.

Given an elliptic curve E modulo P, the number of points on the curve is denoted by #E and is bounded by $p+1-\lfloor 2\sqrt{p} \rfloor \leq E \leq p+1+\lfloor 2\sqrt{p} \rfloor$

- Finding #E is computationally difficult
- so people use, NIST standardised EC's.

"Loving your kids is the best work and caring your parents in turn is the best deed that every child gets a chance to do."

APR 13 2020 MONDAY

Wk 16 (104-262)

All Elliptic curve protocols rely on the hardness of the ECDLP.

If the Elliptic curve is chosen carefully, the best known algorithm for computing the ECDLP requires $\approx \sqrt{P}$ steps.

$P \approx 2^{160}$ requires 2^{80} steps.

The attacks:- Shanks baby-step giant step Pollard's rho method.

Ellipctic curve Diffie Hellman Key Exchange (ECDHKE)

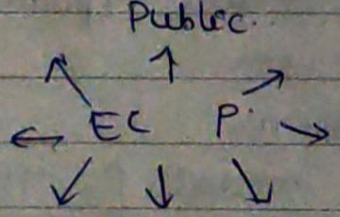
- Straight forward adaption of DH in Z_p.

Phase1: Set-up.

EC - $y^2 \equiv x^3 + ax + b \bmod p$

Primitive Element, generator :- $P = (x_p, y_p)$

Phase 2: Protocol.



Choose $K_{prA} = a \in \{2, 3, \ldots \#E - 1\}$

Compute $K_{pubA} = aP = A = (x_A, y_A)$

A

B.

Choose $K_{prB} = b \in \{2, \ldots \#E - 1\}$

Compute $K_{pubB} = bP = B = (x_B, y_B)$

"Parents are giving up their own dreams to make the dreams of their children come true, so it's now the children's job to take care of their parents well being."

Compute
$aB = T_{AB} = (x_{AB}, y_{AB})$

Compute
$bA = T_{AB} = (x_{AB}, y_{AB})$

Proof: Alice Compute:

$aB = a(bP)$

Bob computes

$bA = b(aP)$

Message

$C = AES_{T_{AB}}(m)$ → $AES^{-1}_{T_{AB}}(C) = m$

Take first 128-bits of the key since $T_{AB} \approx 160$ bits.

Example 6.4:- EC is $y^2 \equiv x^3 + 2x + 12 \bmod 17$, $\#E = 19$, $P = (5,1)$

Alice		Bob
$a = K_{PrA} = 3$		$b = K_{PrB} = 10$
$A = 3P$	A →	$B = 10P$
$= 3(5,1)$		$= (7,11)$
$= (10,6)$	← B	
$T_{AB} = 3(7,11)$		$T_{AB} = 10(10,6)$
$= (13,10)$		$= (13,10)$

"The best deed in the world is the selfless love of the parents for their kids, they want to give them the best security they can, may be in case of humans or animals."

APR 15 2020 WEDNESDAY

Wk 16 (106-260)

Computational Aspects

$a \cdot P$: Q:- How to compute $a \cdot P$ and $b \cdot P$.

There is no direct way to do $a \cdot P$.

$a \cdot P = \underbrace{P + P + \cdots + P}_{a \text{ times}}$

But for large P? what can we do?

In EC?- $a \cdot a = a^2 \longrightarrow$ squaring $P+P$ doubling

$a \cdot x = \longrightarrow P+a \; P+a$ adding

Double and add:

The point multiplication $a \cdot P$ can be computed with the normal "double-add algorithm"

Example 6.5:- $26P = ?$

Caveman way is $P+P+\cdots+P = 26P$.

$26P \equiv (11010)P$.

Step 0:- Compute $P = 1P$

Step 1a:- $P+P = 2P$ 10.P D.

1b:- $2P+P = 3P$ 11.P A

2a:- $3P+3P = 6P$ 110P D

2b:- $6P+6P = 12P$ 1100P D.

3a:- $12P+P = 13P$ 1101.P A

4: $13P+13P = 26P$ - 11010P D.

"If you can feel the importance of cleanliness, then you will never feel low to take steps towards the cleanliness of the society."